Primary Prime Functions in Several Variables and a Generalization of an Important Theorem of Dedekind.

By Harris Hancock.

In the usual theory of numbers, all integers are divided into two classes: the prime numbers and the composite numbers. By a finite number of trials one can determine whether an integer is prime or composite. In the theory of algebraic functions we have to consider whether a polynomial in x with integral coefficients is or is not decomposable into factors, and this determination is also effected by a finite number of trials. Methods of limiting the number of trials have been given by Kronecker,[*] Runge,[†] and Mandl,[‡] who at the same time show how to find the factors when the polynomial is reducible into factors.

The decomposition of polynomials in two or more variables with integral coefficients into their irreducible factors, has been treated by Meyer[||] and the author.[§]

The next problem which we have to consider is the decomposition of polynomials in one variable with integral coefficients into their irreducible factors, when the coefficients are taken with respect to a modulus which is a prime integer. For example, the polynomial

$$f(x) = a_0 x^\tau + a_1 x^{\tau-1} + \dots + a_\tau,$$

where the integers $a_0, a_1, \dots a_\tau$ are taken with respect to the modulus p, is decomposable into factors when it is possible to find three integral functions in x with integral coefficients $f_1(x)$, $f_2(x)$ and $\phi_1(x)$ such that

$$f(x) = f_1(x) f_2(x) + p\phi_1(x),$$

or

$$f(x) \equiv f_1(x) f_2(x) \quad (\text{mod. } p).$$

[*] Kronecker, "Grundzüge," etc., §4, p. 11.

[†] Runge, Crelle, Bd. XCIX, p. 89.

[‡] Mandl, Crelle, Bd. CXIII, p. 252.

[||] Meyer, Math. Ann., Bd. XXX, p. 30.

[§] Hancock, Ann. de l'École Norm. Sup., t. XVII, p. 89.

In this case we say that $f(x)$ is *decomposable into factors* (mod. p); otherwise we say that $f(x)$ is *irreducible* (mod. p).

In Crelle's Journal, Bd. CXXII, p. 269, the author has indicated by a simple example the methods which are to be employed in the general case.

In the same way we may consider a polynomial $F(x, y)$ in two variables with integral coefficients, where the polynomial, when expanded, has the form

$$F(x, y) = a_0(x)\, y^\rho + a_1(x)\, y^{\rho-1} + \ldots. + a_{\rho-1}(x)\, y + a_\rho(x).$$

We suppose that the coefficients $a_0(x), a_1(x), \ldots. \; a_\rho(x)$ are taken with respect to an integral function in x with integral coefficients, $g_1(x)$, say, and that the integral coefficients in $g_1(x)$ have been reduced with respect to the prime integer p. We further assume that $g_1(x)$ is irreducible (mod. p).

We say that $F(x, y)$ is *reducible into factors with respect to the prime integer p and the irreducible* (*mod.* p) *function* $g_1(x)$ when two factors $F_1(x, y)$ and $F_2(x, y)$ can be found so that

$$F(x, y) = F_1(x, y)\, F_2(x, y) + p\phi, (x, y) + g_1(x)\, \psi, (x, y),$$

or

$$F(x, y) \equiv F_1(x, y)\, F_2(x, y) \; [\text{modd. } p, g_1(x)],$$

where $\phi_2(x, y)$ and $\psi_2(x, y)$ are two polynomials integral in x, y, with integral coefficients; otherwise $F(x, y)$ is *irreducible* with respect to the modular system $[p, g_1(x)]$.

In the same manner, if $g_2(x, y)$ is an integral function in x, y with integral coefficients, and is irreducible with respect to the modular system $[p, g_1(x)]$, we say that *a function $G(x, y, z)$ integral in x, y, z with integral coefficients is decomposable into factors with respect to the three moduli, p, $g_1(x)$, $g_2(x, y)$*, when we can find functions $G_1(x, y, z)$, $G_2(x, y, z)$, $\phi_3(x, y, z)$, $\psi_3(x, y, z)$, $\chi_3(x, y, z)$ integral in these variables with integral coefficients such that

$$G(x, y, z) = G_1(x, y, z)\, G_2(x, y, z) + p\phi_3(x, y, z) + g_1(x)\, \psi_3(x, y, z) + g_2(x, y)\, \chi_3(x, y, z),$$

or

$$G(x, y, z) \equiv G_1(x, y, z)\, G_2(x, y, z) [\text{modd. } p, g_1(x), g_2(x, y)].$$

When such functions cannot be found, the function $G(x, y, z)$ is *irreducible* with respect to the modular system $[p, g_1(x), g_2(x, y)]$.

Such conceptions may be extended as far as we choose.

In the first case considered above we have to consider polynomials in one variable taken with respect to the prime integer p as a modulus; in the second case we consider polynomials in two variables with respect to the *prime* modular system $[p, g_1(x)]$, cf. Kronecker (Werke III$^{\text{I}}$, p. 158); in the third case polynomials in three variables with respect to the *prime* modular system $[p, g_1(x), g_2(x, y)]$, etc.

Let us take the polynomial

$$f(x) = a_0 x^\tau + a_1 x^{\tau-1} + \ldots\ldots + a_\tau,$$

when $a_i\,(i = 0, 1, \ldots\ldots \tau)$ are integers that are not divisible by p. Then it is always possible to find two other integers, positive or negative, $\bar{a}_0$ and $\bar{p}$ such that

$$a_0\bar{a}_0 + p\bar{p} = 1.$$

Hence instead of considering functions like $f(x)$ with respect to the modulus p, we may consider the function $a_0 f(x) = f_0(x)$, say, where

$$f_0(x) = 1.\ x^\tau + b_1\, x^{\tau-1} + b_2\, x^{\tau-2} + \ldots\ldots + b_\tau \pmod{p},$$

and the integers $b_1, b_2, \ldots\ldots b_\tau$ have all been reduced (mod. p) and consequently are to be found among the numbers $0, 1, 2, \ldots\ldots p - 1$. For it is seen that if we multiply the function $f_0(x)$ in turn by the complete system of incongruent (mod. p) numbers $1, 2, \ldots\ldots p - 1$, we have the same $p - 1$ functions (mod. p) as we have when $f(x)$ is multiplied by these numbers.

Next write

$$F(x, y) = a_0(x)\, y^\rho + a_1(x)\, y^{\rho-1} + \ldots\ldots + a_\rho(x),$$

where $a_i(x)\, [i = 0, \ldots\ldots \rho]$ are integral functions in x with integral coefficients and consider this function with respect to the modular system $[p, g_1(x)]$.

We assume that none of the function $a_0(x), a_1(x) \ldots\ldots a_\rho(x)$ is divisible by the modular system $[p, g_1(x)]$, that is, we cannot find two functions $\alpha(x)$ and $\beta(x)$ integral in x with integral coefficients so that

$$a_0(x) = p\,\alpha(x) + g_1(x)\,\beta(x).$$

This assumption granted, since $g_1(x)$ can have no factor in common with $a_0(x)$, it is always possible to find two functions $\bar{a}_0(x)$ and $\bar{g}_1(x)$ integral in x with integral coefficients, such that

$$a_0(x)\,\bar{a}_0(x) + g_1(x)\,\bar{g}_1(x) = m,$$

where m is an integer.

We can further find two integers $\overline{m}$ and π so that

$$m\overline{m} = 1 + p\pi.$$

Hence
$$\overline{m}\,a_0(x)\,\overline{a}_0(x) + \overline{m}\,g_1(x)\,\overline{g}_1(x) = 1 + p\pi,$$
and finally
$$\overline{m}\,\overline{a}_0(x)\,a_0(x) \equiv 1 \ [\text{mod.}\, p, g_1(x)].$$

Consequently writing $\overline{m}\,\overline{a}_0(x)\,F(x,y) = F_0(x, y)$, we have

$$F_0(x, y) = 1\, y^\rho + b_1(x)\,y^{\rho-1} + \ldots. + b_\rho(x) \ [\text{modd.}\, p,\, g_1(x)].$$

By means of the function $g_1(x)$ the degrees of the functions $b_1(x), \ldots. b_\rho(x)$ have all been reduced so as to be less than the degree of $g_1(x)$ and owing to the presence of p, all the numerical coefficients that appear are less than this prime integer.

Suppose next that

$$g_1(x) = 1.\ x^{n_1} + \gamma_1 x^{n_1-1} + \gamma_2 x^{n_1-2} + \ldots. + \gamma_{n_1-1} x + \gamma_{n_1},$$

where the integers $\gamma_1, \gamma_2, \ldots. \gamma_{n_1-1}, \gamma_{n_1}$ are found among the integers 0, 1, 2, $\ldots. p - 1$.

By giving in turn these p values to each of the integers $\gamma_1, \gamma_2, \ldots. \gamma_{n_1}$ we derive $p^{n_1} = p_1$, say, functions which form the complete system of incongruent residues with respect to the modular system $[p, g_1(x)]$.

If we multiply the function $F_0(x, y)$ in turn by the $\varkappa = p^{n_1} - 1$ functions other than $g_1(x)$ we derive the same system of functions with respect to the modular system $[p, g_1(x)]$ as is had when we multiply the original function $F(x, y)$ by this same system of functions (cf. Crelle's Journal, Bd. CXXII, p. 271).

Proceeding in the same manner let $g_2(x, y)$ be an irreducible function with respect to the moduli p, $g_1(x)$, and with respect to the prime modular system $[p, g_1(x), g_2(x, y)]$ consider the function

$$G(x, y, z) = a_0(x, y)\,z^\sigma + a_1(x, y)\,z^{\sigma-1} + \ldots. + a_\sigma(x, y),$$

where $a_0(x, y), a_1(x, y), \ldots. a_\sigma(x, y)$ are integral functions in x, y with integral coefficients and are not divisible by the modular system $[p, g_1(x), g_2(x, y)]$.

We can always determine a multiplier $m_1\,\phi_1(x)\,\overline{a}_0(x, y)$, where m_1 is an integer, $\phi_1(x)$ is an integral function in x with integral coefficients and $\overline{a}_0(x, y)$ is an integral function in x, y with integral coefficients such that

$$m_1\phi_1(x)\,\overline{a}_0(x, y)\,a_0(x, y) \equiv 1 \ [\text{modd.}\, p, g_1(x), g_2(x, y)].$$

Consequently if we write $m\phi_1(x)\overline{a_0}(x, y)\ G(x, y, z) = G_0(x, y, z)$, it is seen that $G_0(x, y, z)$ has the form

$$G_0(x, y, z) \equiv z^\sigma + b_1(x, y)\, z^{\sigma-1} + b_2(x, y)\, z^{\sigma-2} + \ldots. \\ + b_\sigma(x, y)\ [\text{modd. } p, g_1(x), g_2(x, y)],$$

where $b_1(x, y), b_2(x, y), \ldots. b_\sigma(x, y)$ have been reduced with respect to the modular system $[p, g_1(x), g_2\, x, y)]$.

Suppose next that with respect to the modular system $[p, g_1(x)]$ that the function $g_2(x, y)$ has the form

$$g_2(x, y) = 1y^{n_2} + \delta_1(x)\, y^{n_2-1} + \delta_2(x)\, y^{n_2-2} + \ldots. + \delta_{n_2}(x),$$

where $\delta_1(x), \delta_2(x), \ldots. \delta_{n_2}(x)$ may be any of the p^{n_1} functions that constitute the complete system of incongruent residues with respect to the modular system $[p, g_1(x)]$.

There are consequently $[p^{n_1}]^{n_2} = p^{n_1 n_2} = p_2$ (say) such functions of the form $g_2(x, y)$ including, of course, the function $g_2(x, y)$ itself, and these p_2 functions constitute with respect to the modular system $[p, g_1(x), g_2(x, y)]$ a complete system of incongruent residues. It is also seen that the function $G(x, y, z)$ when multiplied in turn by the $p_2 - 1$ functions other than $g_2(x, y)$ produces the same system of functions with respect to the modular system $[p, g_1(x), g_2(x, y)]$ as those derived by the multiplication of $G_0(x, y, z)$ by the same system of functions.

Continuing this process let us form modular systems as follows: let p be a prime integer; then let $g_1(x_1)$ be an irreducible (mod. p) function of the n_1 degree in x_1 (all constant coefficients are once for all assumed integral); let $g_2(x_1, x_2)$ be irreducible [modd. p, $g_1(x_1)$] and of the n_2 degree in x_2 and form the modular system $[p, g_1(x_1), g_2(x_1, x_2)]$; let $g_3(x_1, x_2, x_3)$ be irreducible [modd. p, $g_1(x_1)$, $g_2(x_1, x_2)$] and of the n_3 degree in x_3, etc.

We may thus form the modular system

$$[M] = [p, g_1(x_1), g_2(x_1, x_2), \ldots. g_m(x_1, x_2, \ldots. x_m)].$$

With respect to this modular system there are a system of $p^{n_1 n_2 \ldots. n_m} = p_m$ incongruent residues which we may denote by $r_1(x_1, x_2, \ldots. x_m)$, $r_2(x_1, x_2, \ldots. x_m)$, $\ldots.\ r_{p_m}(x_1, x_2, \ldots. x_m)$, of which one is the function $g_m(x_1, x_2, \ldots. x_m)$ itself.

With respect to these residues and the above modular system, there exist the same relations for the integral functions in these m variables as those expressed by the theorems of Fermat, Wilson, etc., in the theory of rational whole numbers, where the integers are taken with respect to a prime integer as modulus. Indeed, all the theorems given in §§26–31 of Dirichlet's "Zahlentheorie" (Dedekind, 4th edition), regarding congruences, primitive roots, etc., have their exact analogons here.

We come next to the consideration of functions $f(x_1, x_2, \ldots., x_m, x)$ taken with respect to the modular system $[M]$.

As above, it is seen that we may multiply this function by another function $\bar{f}(x_1, x_2, \ldots., x_m)$ say, so that when expanded in descending powers of x, the function $\bar{f}(x_1, x_2, \ldots. x_m)\, f(x_1, x_2, \ldots. x_m, x) = F(x_1, x_2, \ldots. x_m, x)$ has the form

$$F(x_1, x_2, \ldots. x_m, x) = 1 . x^\pi + a_1(x_1, x_2, \ldots. x_m)\, x^{\pi-1} + \ldots. \\ + a_\pi(x_1, x_2, \ldots. x_m).$$

Such functions may be called *primary* functions in the $m+1$ variables $x_1, x_2, \ldots. x_m, x$.

Regarding primary functions in one variable, see Galois (Journal de Math., t. XI, p. 398) Dedekind (XI Supplement to Dirichlet's "Zahlentheorie," p. 571 and other references of his works there cited; also, the numerous applications in C. Jordan's "Traité des Substitutions," Paris, 1870).

The first question which presents itself is: *to determine the number of primary functions in which the variable x occurs to the π^{th} degree, which are irreducible with respect to the modular system* $[M]$. Such functions are called *primary prime* functions.

The question may be expressed as follows: *to determine the number of primary prime functions that exist with respect to a given prime modular system, when the variable that does not appear in the modular system is of a given degree π, say.*

When $\pi = 1$, the function in question is

$$1)\quad x + a(x_1, x_2, \ldots. x_m),$$

where $a(x_1, x_2, \ldots. x_m)$ is an integral function in the variables and has been reduced by means of the modular system $[M]$.

There are consequently $p^{n_1 \cdot n_2 \cdots\cdot n_m} = p_m$ such functions, viz., the functions that are had when for $a(x_1, x_2, \ldots. x_m)$ is replaced each of the p_m functions $r_1(x_1, x_2, \ldots. x_m)$, $r_2(x_1, x_2, \ldots. x_m)$, $\ldots.$ $r_{p_m}(x_1, x_2, \ldots. x_m)$.

If we denote by ω_1 the number of primary prime functions, where $\pi = 1$, we have*

$$\omega_1 = p_m.$$

When $\pi = 2$, we have the primary functions of the second degree in x, the form being

$$2) \quad x^2 + a(x_1, x_2, \ldots . x_m)x + b(x_1, x_2, \ldots . x_m),$$

where, in the places of $a(x_1, x_2, \ldots . x_m)$ and $b(x_1, x_2, \ldots . x_m)$, there may occur any of the p_m functions $r_1(x_1, x_2, \ldots . x_m), \ldots .$

There are consequently p_m^2 functions of the form 2), that is, primary functions of the second degree in x, where the coefficients have been reduced with respect to the modular system $[M]$.

To determine which of these functions are prime, we have only to subtract from p_m^2 the number of primary functions which arise from the multiplication of two primary functions of the first degree. This number is, since repetitions are allowable, $\frac{p_m(p_m+1)}{2}$. Hence, if ω_2 denotes the number of primary prime functions of the second degree in x whose coefficients have been reduced with respect to the modular system $[M]$, we have

$$\begin{aligned}\omega_2 &= p_m^2 - \frac{p_m(p_m+1)}{2} \\ &= \tfrac{1}{2}p_m(p_m-1).\end{aligned}$$

A primary function of the third degree in x has the form

$$x^3 + a(x_1, x_2, \ldots . x_m)x^2 + b(x_1, x_2, \ldots . x_m)x + c(x_1, x_2, \ldots . x_m),$$

and we have all primary functions of the third degree in x whose coefficients have been reduced with respect to the modular system $[M]$ when, in the places of the functions $a(x_1, x_2, \ldots . x_m)$, $b(x_1, x_2, \ldots . x_m)$ and $c(x_1, x_2, \ldots . x_m)$, we substitute any of the p_m functions $r_1(x_1, x_2, \ldots . x_m), \ldots .$

We thus have p_m^3 such primary functions. These functions are either prime functions or products of a prime function of the first degree and one of the second degree or products of three primary prime functions of the first degree.

* The present method is similar to that employed in the lectures at Berlin in 1894 on "Zahlentheorie," 2nd Part, by Professor George Frobenius for functions in one variable. I take the opportunity here of thanking this eminent mathematician for his courtesy in allowing me to make use of these lectures.

The number of the products of a primary prime function of the first degree with a primary prime function of the second degree is $\omega_1 \omega_2$; and the number of the products of any three primary prime functions of the first degree is equal to the number of combinations of p_m elements taken three at a time admitting repetitions, that is, equal to $\frac{p_m (p_m + 1)(p_m + 2)}{1 . 2 . 3}$.

Hence, denoting the number of primary prime functions of the third degree in x whose coefficients have been reduced with respect to the modular system $[M]$ by ω_3, we have

$$p_m^3 = \omega_3 + \omega_1 \omega_2 + \frac{p_3 (p_m + 1)(p_m + 2)}{1 . 2 . 3},$$

from which it follows that

$$\begin{aligned} \omega_3 &= p_m^3 - \frac{p_m \cdot p_m (p_m - 1)}{2} - \frac{p_m (p_m + 1)(p_m + 2)}{6} \\ &= \frac{p_m^3 - p_m}{3} . \end{aligned}$$

We go now to the general determination of the number of the primary prime functions of the degree h in the variable x whose coefficients have been reduced with respect to the modular system $[M]$.

The number of primary functions of the degree h is p_m^h, since each of the h coefficients of the primary functions may be replaced by any of the functions

$$r_1 (x_1, x_2, \ldots . x_m), \; r_2 (x_1, x, \ldots . x_m), \; \ldots . \; r_{p_m} (x_1, x_2, \ldots . x_m).$$

Such a primary function of degree h can be either a primary prime function of the degree h or a product of a primary prime functions of the first degree, b primary prime functions of the second degree, c primary prime functions of the third degree, etc., where $a, b, c, \ldots .$ are arbitrary integers $(\geqq 0)$ which are subjected to the only condition that

$$a + 2b + 3c + \ldots . = h.$$

Now in how many different ways is such a formation of a product of a primary prime functions of the first degree, b primary prime functions of the second degree, etc., possible?

There are ω_1 primary prime functions of the first degree; these may be combined taken together a at a time and allowing repetitions in

$$\frac{\omega_1(\omega_1+1)(\omega_1+2)\ \ldots\ldots\ (\omega_1+a-1)}{1.\,2.\,3.\ \ldots\ldots\ a},$$

different ways. Similarly the ω_2 primary prime functions of the second degree may, when b of them are taken together and allowing repetitions, be combined in

$$\frac{\omega_2(\omega_2+1)(\omega_2+2)\ \ldots\ldots\ (\omega_2+b-1)}{1.\,2.\,3.\ \ldots\ldots\ b}.$$

ways, etc.

Hence a product of a primary prime functions of the first degree, b primary prime functions of the second degree, etc., can be formed in

$$\frac{\omega_1(\omega_1+1)\ \ldots\ldots\ (\omega_1+a-1)}{a\,!}\cdot\frac{\omega_1(\omega_1+1)\ \ldots\ldots\ (\omega_1+b-1)}{b\,!}\ \ldots\ldots$$

ways.

We define the symbol $\binom{x}{n}$ by the well known relation,

$$\binom{x}{n}=\frac{x(x-1)(x-2)\ \ldots\ldots\ (x-n+1)}{n\,!},$$

where x is quite arbitrary, while n is a positive integer.

By means of this symbol we may write the above product in the form

$$(-1)^a\binom{-\omega_1}{a}(-1)^b\binom{-\omega_2}{b}\cdots\cdots$$

If we take the summation of this product over all systems of numbers $a, b, c, \ldots\ldots$ which satisfy the relation

$$a+2b+3c+\ \ldots\ldots\ =h,$$

we have the number of all primary functions of degree h, i. e.

$$p_m^h=\sum\left\{(-1)^a\binom{-\omega_1}{a}(-1)^b\binom{-\omega_2}{b}\ \cdots\cdots\right\},$$

where the summation is to be taken over all systems of numbers $a, b, c, \ldots\ldots$ which satisfy the condition

$$a+2b+3c+\ \ldots\ldots\ =h.$$

Let x be a variable; we then have

$$x^a\, x^{2b}\, x^{3c} \ldots\ldots = x^h,$$

and if we multiply the above expression by x^h, it follows that

$$(p_m\, x)^h = \sum \left\{ (-1)^a \binom{-\omega_1}{a} x^a\, (-1)^b \binom{-\omega_2}{b} x^{2b} \ldots\ldots \right\},$$

where the summation is to be taken as before.

This formula is true for all values of

$$h = 0,\ +1,\ +2, \ldots\ldots \textit{ ad infinitum.}$$

If y is an arbitrary variable, whose absolute value is < 1, then is

$$\frac{1}{1-y} = \sum_{h=0}^{h=\infty} y^h.$$

Accordingly, if we assume that $p_m |x| < 1$, then is

$$\frac{1}{1-p_m x} = \sum_{h=0}^{h=\infty} p_m^h x^h,$$

and, consequently,

$$\frac{1}{1-p_m x} = \sum_{h=0}^{h=\infty} \Big[\sum_{a,\, b,\, c,\, \ldots\ldots} \left\{ (-1)^a \binom{-\omega_1}{a} x^a (-1)^b \binom{-\omega_2}{b} x^{2b} \ldots\ldots \right\} \Big],$$
$$(a + 2b + 3c + \ldots\ldots = h),$$

or $$\frac{1}{1-p_m x} = \sum_{(a)} \left\{ (-1)^a \binom{-\omega_1}{a} x^a \right\} \cdot \sum_{(b)} \left\{ (-1)^b \binom{-\omega_2}{b} x^{2b} \right\} \ldots\ldots,$$

since, in this manner for the above double summation, we may write a product of an infinite number of single summations owing to the convergence of the series. Further, since, in the double summation, h is taken from 0 to ∞, it follows also in the single summations that we must also cause the summations to be made from 0 to ∞. From the binomial theorem it follows that

$$(1-x)^{-\omega_1} = \sum_{a=0}^{\infty} \left\{ (-1)^a \binom{-\omega_1}{a} x^a \right\},$$

$$(1-x^2)^{-\omega_2} = \sum_{b=0}^{\infty} \left\{ (-1)^b \binom{-\omega_2}{b} x^{2b} \right\},$$

$$(1-x^3)^{-\omega_3} = \sum_{c=0}^{\infty} \left\{ (-1)^c \binom{-\omega_3}{c} x^{3c} \right\},$$

etc.

Consequently, we have

$$1 - p_m x = (1 - x)^{\omega_1} (1 - x^2)^{\omega_2} (1 - x^3)^{\omega_3} \dots\dots$$
$$= \prod_{d=1}^{\infty} \left\{ (1 - x^d)^{\omega_d} \right\}.$$

From this equation we may easily determine the quantities ω_1, ω_2, ω_3, ... *ad infinitum, by equating like powers of* x.

We further have from this relation

$$\log (1 - p_m x) = \log \prod_{d=1}^{\infty} \left\{ (1 - x^d)^{\omega_d} \right\}$$
$$= \sum_{d=1}^{\infty} \left\{ \log (1 - x^d)^{\omega_d} \right\}$$
$$= \sum_{d=1}^{\infty} \left\{ \omega_d \log (1 - x^d) \right\}.$$

If we differentiate this equation with respect to x, we have

$$\frac{p_m}{1 - p_m x} = \sum_{d=1}^{\infty} \left\{ d\omega_d \frac{x^{d-1}}{1 - x^d} \right\};$$

and, multiplying by x, it follows that

$$\frac{p_m x}{1 - p_m x} = \sum_{d=1}^{\infty} \left\{ d\omega_d \frac{x^d}{1 - x^d} \right\}.$$

But, owing to the identical relation,

$$\frac{x^d}{1 - x^d} = \sum_{n=1}^{\infty} x^{dn},$$

the above equation becomes

$$\frac{p_m x}{1 - p_m x} = \sum_{d=1}^{\infty} \left\{ d\omega_d \sum_{n=1}^{\infty} x^{dn} \right\}$$
$$= \sum_{n=1}^{\infty} \left\{ \sum_{d=1}^{\infty} d\omega_d \, x^{dn} \right\}.$$

On the other hand we have

$$\frac{p_m x}{1 - p_m x} = \sum_{h=1}^{\infty} (p_m^h x^h),$$

and consequently it follows that

$$\sum_{n=1}^{\infty}\left\{\sum_{d=1}^{\infty}(d\omega_d\, x^{dn})\right\} = \sum_{h=1}^{\infty}(p_m^h\, x^h).$$

Since this equation must exist identically, we have by equating like powers of x on either side, the relation

$$p_m^h = \sum_{(d)} d\omega_d\ ,$$

where, in the summation d is to be taken over all values for which $h = d_n$, that is, d is taken over all divisors of h, including h.

An immediate application of the above results is to be found in an extension of a theorem due to Dedekind, a theorem which in the further development of the theory of algebraic numbers will hold the same important position as do the theorems of Fermat and Wilson in the ordinary theory of rational numbers.

Consider the algebraic numbers that belong to a fixed realm of rationality* (Körper), which denote by Ω and let v be the totality (Dedekind, p. 537) of all the algebraic integers of the realm of rationality Ω.

This modul v (see Dedekind, p. 537) has the same relations with respect to the realm Ω as unity has in the realm of rational numbers, for example

$$v.v = v,$$

$$\frac{v}{v} = v,$$

and every algebraic integer in Ω is divisible by the modul v.

Further let p be a rational prime integer that is divisible by the prime ideal $\mathfrak{p}$ [in v] (Dedekind, p. 560).
Then the norm of $\mathfrak{p}$ is

$$N(\mathfrak{p}) = p^f,$$

where f is a rational integer such that

$$0 < f \leq n,$$

n being the degree of the realm Ω (Dedekind, p. 565).

* Dedekind, XI Supplement to Dirichlet's "Zahlentheorie," fourth edition, p. 452. We shall in the following refer to this supplement by using merely the name of the author.

The number f is called the degree of the ideal $\mathfrak{p}$.

If $\mathfrak{a}$ and $\mathfrak{b}$ are two arbitrary moduls, then the number of classes into which the algebraic integers that are contained in $\mathfrak{a}$ may be distributed with respect to $\mathfrak{b}$ is represented by the symbol[*]

$$(\mathfrak{a}, \mathfrak{b}) = m, \text{ say.}$$

If we choose a definite integer out of each class, we have a complete *representative system* of the modul $\mathfrak{a}$ with respect to the modul $\mathfrak{b}$.

These m integers may be denoted by $\rho_1, \rho_2, \dots \rho_m$. They have the following characteristics:

1) Each of the m numbers is divisible by $\mathfrak{a}$.

2) The difference of any two of these numbers is not divisible by $\mathfrak{b}$.

3) Every number that is divisible by $\mathfrak{a}$ is congruent to one of these m numbers (mod. $\mathfrak{b}$).

Dedekind (p. 564) shows that

$$(v, \mathfrak{p}) = N(\mathfrak{p}) = p^f.$$

Let $p^f = \kappa$ and let $\rho_1, \rho_2, \dots \rho_\kappa$ be a complete representative system of the integers contained in the modul v with respect to the modul $\mathfrak{p}$. As unity is to be found among the integers in v, we take unity as the representative of the class to which it belongs and write one of the numbers $\rho_1, \rho_2, \dots \rho_\kappa$ equal to unity, say $\rho_1 = 1$.

Dedekind (p. 570) further shows, if ω is any algebraic integer in Ω, that

$$\omega^p \equiv \omega \text{ (mod. } \mathfrak{p}).$$

The following theorem follows at once:

$$x^{p-1} - 1 \equiv \Pi (x - \omega) \text{ (mod. } \mathfrak{p}),$$

where x is a variable and the product is to be taken over a system of integers incongruent and relative prime to $\mathfrak{p}$.

Since this congruence exists identically for all values of x, we have, when $x = 0$, the analogon of Wilson's theorem in the theory of rational numbers:

$$\Pi\omega = -1 \text{ (mod. } \mathfrak{p}),$$

[*] Dedekind, p. 509.

where the product is to be taken over a complete system of integers ω which are incongruent (mod. $\mathfrak{p}$) and are relative prime to $\mathfrak{p}$.

If α is an algebraic integer in Ω, and if

$$\alpha^{p^h} \equiv \alpha \ [\text{mod. } \mathfrak{p}],$$

where h is the smallest rational integer that satisfies this congruence, then h is called the *height* (Dedekind, p. 571) of the integer α with respect to the modulus $\mathfrak{p}$.

It is clear that $h \leqq f$.

Consider the infinite series of numbers

$$\alpha^{p^0}, \alpha^{p^1}, \alpha^{p^2}, \alpha^{p^3}, \ldots.$$

with respect to the modulus $\mathfrak{p}$, and let h be the height of α. The first h of these numbers are incongruent (mod. $\mathfrak{p}$), and it is seen that after the first h of these numbers, the next h of them are repeated in the same sequence, etc.

The h numbers $\qquad \alpha^{p^0}, \alpha^{p^1}, \alpha^{p^2}, \ldots. \alpha^{p^{h-1}}$

are called the *period* of the number α.

It may be proved that the congruence

$$x^{p^h} - x \equiv 0 \ (\text{mod. } \mathfrak{p})$$

has exactly p^h incongruent (mod. $\mathfrak{p}$) roots; and, indeed, this congruence is satisfied by all quantities α whose height is h or a divisor of h, the number of such quantities being p^h.

We therefore have

$$1) \quad x^{p^h} - x \equiv \Pi (x - \alpha) \ (\text{mod. } \mathfrak{p}),$$

where the product is to be taken over a system of p^h incongruent (mod. $\mathfrak{p}$) integers whose height is h or a divisor of h.

In this product there appears, if α is an integer whose height is h, the product

$$(x - \alpha)(x - \alpha^p)(x - \alpha^{p^2}) \ldots. (x - \alpha^{p^{h-1}}),$$

a product which we may replace by a congruent (mod. $\mathfrak{p}$) primary prime function of the hth degree in x with rational integral coefficients.

In the same way, there enters in the product 1) a product of the form

$$(x-\beta)(x-\beta^{p})(x-\beta^{p^2})\ \ldots\ldots\ (x-\beta^{p^{d-1}}),$$

if β is an integer whose height is d; this latter product may also be replaced by a congruent (mod. $\mathfrak{p}$) primary prime function of degree d with rational integral coefficients.

It is thus seen that

$$x^{p^h}-x\equiv\Pi P(x)\ \text{(mod. }\mathfrak{p}),$$

where, since $p^h=\sum\limits_{(d)}d\omega_d$, the product is to be taken over all the existing primary prime functions whose height is h or a divisor of h (Dedekind, p. 572).

The preceding investigations have been made for algebraic integers in the fixed realm of rationality Ω. We denote the realm containing all these integers by $[v]$.

Instead of considering algebraic integers we shall now consider integral functions of several variables x_1, x_2, ... x_m whose coefficients are those algebraic integers. We say that such functions belong to the realm of integrity $[v, x_1, x_2, \ldots\ldots x_m]$, this realm being composed of all integral functions in these variables with constant coefficients that belong to the realm $[v]$.

Let us consider first the functions belonging to the realm $[v, x_1]$ and sup pose that

$$f(x_1)=\alpha_0 x_1^n+\alpha_1 x_1^{n-1}+\ldots\ldots+\alpha_n,$$

where $\alpha_0, \alpha_1, \ldots\ldots \alpha_n$ are algebraic integers in the realm $[v]$.

Taken with respect to the prime ideal $\mathfrak{p}$, the algebraic integers in v may be distributed, as shown above, into

$$(v, \mathfrak{p})=p^f=\varkappa \text{ classes.}$$

Further since the norm of $\mathfrak{p}$, that is $N(\mathfrak{p})=\varkappa$, it follows that the rational integers $N(\rho_1)$, $N(\rho_2)$, ... $N(\rho_\kappa)$ are all less than $\varkappa$, the algebraic integers $\rho_1, \rho_2, \ldots\ldots \rho_\kappa$ being as defined above.

In another paper* the author has shown that one of the representatives ρ_i, say, is such that

$$\rho_i\,\alpha_0\equiv 1\ \text{(mod. }\mathfrak{p}),$$

* Mémoire sur les systèmes modulaires de Kronecker (Ann. de l'École Norm. Sup., t. XVIII, Supplement I, p. 64).

and further with respect to the modulus $\mathfrak{p}$, we have the same system of functions when we multiply the function $f(x_1)$ in turn by the numbers $\rho_1, \rho_2, \ldots\ldots \rho_\kappa$ as we have when the function $\rho_i f(x_1)$ is multiplied by this same system of numbers. Hence instead of considering the original function $f(x_1)$ with respect to the modulus $(\mathfrak{p})$, we may consider the function $f_0(x_1) = \rho_i f(x_1)$ with respect to this modulus.

The function $f_0(x_1)$ has the form

$$f_0(x_1) = x_1^n + \overline{\alpha}_1 x_1^{n-1} + \overline{\alpha}_2 x_1^{n-2} + \ldots\ldots + \overline{\alpha}_n,$$

where $\overline{\alpha}_1, \overline{\alpha}_2, \ldots\ldots \overline{\alpha}_n$ are to be found among the integers $\rho_1, \rho_2, \ldots\ldots \rho_\kappa$.

It is clear that the number of functions having the form $f_0(x_1)$ is $\varkappa^n$.

This then is the number of incongruent functions of degree n in the realm $[v, x_1]$ with respect to the modulus $\mathfrak{p}$ and these functions together with the prime ideal $\mathfrak{p}$ constitute the modular system

$$[\mathfrak{p}, f_0(x_1)].$$

Next, suppose that $g_1(x_1)$ is an irreducible function with respect to the modulus $\mathfrak{p}$ and is of the form

$$g_1(x_1) = x_1^{n_1} + \beta_1 x_1^{n_1-1} + \beta_2 x_1^{n_1-2} + \ldots\ldots + \beta_{n_1},$$

where $\beta_1, \beta_2, \ldots\ldots \beta_{n_1}$ are to be found among the integers $\rho_1, \rho_2, \ldots\ldots \rho_\kappa$.

Let us form the prime modular system

$$[\mathfrak{p}, g_1(x_1)].$$

Then the number of incongruent (modd. $\mathfrak{p}$, $g_1(x_1)$) functions in the realm $[v, x_1]$ is x^{n_1}.

Let $\phi(x_1, x_2)$ be an integral function in x_1, x_2 with integral coefficients that belong to $[v]$, and when expanded in descending powers of x_2 suppose that the form of $\phi(x_1, x_2)$ is

$$\phi(x_1, x_2) = d_0(x_1) x_2^\gamma + d_1(x_1) x_2^{\gamma-1} + \ldots\ldots + d_\gamma(x_1).$$

With respect to the modular system $[\mathfrak{p}, g_1(x_1)]$ we may always find a function $\overline{d_0}(x_1)$ integral in x_1 with coefficients that belong to $[v]$ such that

$$\overline{d_0}(x_1) d_0(x_1) \equiv 1 \ [\text{modd. } \mathfrak{p}, g_1(x_1)].$$

Hence, with respect to this modular system, the function $\overline{d_0}(x_1)\phi(x_1, x_2) = \phi_0(x_1, x_2)$ is of the form

$$\phi_0(x_1, x_2) = x_2^\gamma + \overline{d_1}(x_1)x_2^{\gamma-1} + \overline{d_2}(x_1)x_2^{\gamma-2} + \dots + d_\gamma(x_2),$$

where the functions $\overline{d_1}(x_1)$, $\overline{d_2}(x_1)$, ... $\overline{d}_\gamma(x_2)$ belong to the realm $[v, x_1]$ and are of degrees at most $= n_1 - 1$ in x_1.

Consequently, the number of functions of this form is $\varkappa^{n_1\gamma}$, and these functions form a system of incongruent residues in the realm $[v, x_1, x_2]$ with respect to the modular system $[\mathfrak{p}, g_1(x_1), \phi_0(x_1, x_2)]$.

Next suppose that, taken with respect to the modular system $[\mathfrak{p}, g_1(x_1)]$, the function

$$g_2(x_1, x_2) = x_2^{n_2} + \beta_1(x_1)x^{n_2-1} + \beta_2(x_1)x^{n_2-2} + \dots + \beta_{n_2}(x_1)$$

is irreducible, and form the prime modular system

$$[\mathfrak{p}, g_1(x_1), g_2(x_1, x_2)].$$

With respect to this modular system, the number of incongruent functions in the realm $[v, x_1, x_2]$ is $\varkappa^{n_1 \cdot n_2}$.

Continuing this process, let

$$g_3(x_1, x_2, x_3) = x_3^{n_3} + \gamma_1(x_1, x_2)x_3^{n_3-1} + \dots + \gamma_{n_3}(x_1, x_2)$$

be an irreducible function with respect to the modular system $[\mathfrak{p}, g_1(x_1), g_2(x_1, x_2)]$ where the coefficients $\gamma_1(x_1, x_2)$, ... $\gamma^{n_3}(x_1, x_2)$ belong to the realm $[v, x_1, x_2]$.

Then, with respect to the prime modular system

$$[\mathfrak{p}, g_1(x_1), g_2(x_1, x_2), g_3(x_1, x_2, x_3)],$$

there are $\varkappa^{n_1 \cdot n_2 \cdot n_3}$ incongruent functions in the realm $[v, x_1, x_2, x_3]$.

By extending this process, we form the prime modular system

$$[M] \quad [\mathfrak{p}, g_1(x_1), g_2(x_1, x_2), g_3(x_1, x_2, x_3), \dots g_m(x_1, x_2, \dots x_m)],$$

where the function $g_i(x_1, x_2, \dots x_i)$ is irreducible with respect to the modular system $[p, g_1(x_1), g_2(x_1, x_2), \dots g_{i-1}(x_1, x_2, \dots x_{i-1})]$,

$$(i = 2, 3, \dots m)$$

and is of degree n_i in x_i.

Then with respect to the modular system $[M]$ there are $\kappa^{n_1 \cdot n_2 \cdots\cdots n_m}$ incongruent functions in the realm $[v, x_1, x_2, \ldots\ldots x_m]$.

For brevity write

$$\kappa_i = \kappa^{n_1 \cdot n_2 \cdots\cdots n_i} (i = 1,\ 2,\ \ldots\ldots m)$$

and let us denote the above residues by

$$r_1(x_1, x_2, \ldots\ldots x_m),\ r_2(x_1, x_2, \ldots\ldots x_m),\ \ldots\ldots r_{\kappa_m}(x_1, x_2, \ldots\ldots x_m),$$

of which one is the function $g_m(x_1, x_2, \ldots x_m)$.

Omitting for the moment this residue from the consideration, it is seen that if $\zeta(x_1, x_2, \ldots\ldots x_m)$ is any quantity belonging to the realm $[v, x_1, x_2, \ldots\ldots x_m]$ then is

$$[\zeta(x_1, x_2, \ldots\ldots x_m]^{\kappa_m - 1} \equiv 1\ [\text{modd. } \mathfrak{p},\ g_1(x_1) \ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)].$$

THEOREM. *If r is any of the above residues $r_1, r_2, \ldots\ldots r_{\kappa_m}$, where we have used the functional signs instead of the functions themselves and if*

$$G(r) = A_0 r^{\nu} + A_1 r^{\nu-1} + \ldots\ldots$$
$$+ A_{\nu} \equiv 0\ [\text{modd. } \mathfrak{p},\ g_1(x_1),\ g_2(x_1, x_2),\ \ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)],$$

where $A_0, A_1, \ldots\ldots A_{\nu}$ are functions of the realm $[v, x_1, x_2, \ldots\ldots x_m]$, and if further $A_0 \not\equiv 0$ [modd. $\mathfrak{p}$, $g_1(x_1), \ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)$], then the congruence 1) *cannot have more than ν incongruent* [modd. $\mathfrak{p}$, $g_1(x_1)$, $g_2(x_1, x_2)$, $\ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)$] *roots ; if further*

$$G(r) \equiv 0\ [\text{modd. } \mathfrak{p},\ g_1(x_1),\ g_2(x_1, x_2),\ \ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)],$$

has exactly ν incongruent roots $R_1, R_2, \ldots\ldots R_{\nu}$, say, with respect to this modular system, we have the identical congruence

$$G(r) \equiv A_0 \prod_{i=1}^{i=\nu} (r - R_i)\ (\text{modd. } \mathfrak{p},\ g_1(x_1),\ g_2(x_1, x_2),\ \ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)].$$

Hence since

$$r^{\kappa_m} - r \equiv 0\ [\text{modd. } \mathfrak{p},\ g_1(x_1),\ g_2(x_1, x_2), \ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)],$$

has the κ_m incongruent [modd. $\mathfrak{p}$, $g_1(x_1)$, $g_2(x_1, x_2)$, $\ldots\ldots g_m(x_1, x_2, \ldots\ldots x_m)$] roots $r_1, r_2, \ldots\ldots r_{\kappa_m}$ above, it is seen that we have the identical congruence:

$$r^{\kappa_m - 1} - 1 \equiv \prod_{\lambda} (r - r_\lambda) \; [\text{modd. } \mathfrak{p}, g_1 (x_1) \, g_2, (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)]$$

where the congruence is to be taken over the $\kappa_m - 1$ residues $r_1, r_2, \ldots r_{\kappa_m}$ not including $g_m (x_1, x_2, \ldots x_m)$.

Equating the coefficients of r on either side of this congruence, we have the very general *Wilson Theorem*

$$-1 \equiv \prod_{\lambda} r_\lambda \; [\text{modd. } \mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)],$$

where the product is to be taken as above.

Let $\xi (x_1, x_2, \ldots x_m)$ be any quantity of the realm $[v, x_1, x_2, \ldots x_m]$ so that therefore

$$[\xi (x_1, x_2, \ldots x_m)]^{\kappa_m} \equiv \xi (x_1, x_2, \ldots x_m)$$
$$[\text{modd. } \mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)].$$

Hence if we write the functional sign for the function itself and give to κ_m its value $p^{f \cdot n_1 \cdot n_2 \ldots n_m} = p^f_m$, then is

$$[\xi]^{p^f_m} \equiv \xi \; [\text{modd. } \mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)].$$

Following the analogy of Dedekind we may call h the *height* of the function $\eta (x_1, x_2, \ldots x_m)$ with respect to the modular system $[\mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)]$ when h is the smallest rational integer such that $[\eta]^{p^h_m} \equiv \eta \; [\text{modd. } \mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)]$ and consequently $h \leq f$.

The functions

$$\eta^{p^0_m}, \eta^{p^1_m}, \eta^{p^2_m}, \ldots \eta^{p^{h-1}_m},$$

constitute the period of the function η with respect to the modular system $[\mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)]$.

The product

$$(x - \eta^{p^0_m})(x - \eta^{p_m})(x - \eta^{p^2_m}) \ldots (x - \eta^{p^{h-1}_m}),$$

is congruent to

$$P (x, x_1, x_2, \ldots x_m) \; [\text{modd. } \mathfrak{p}, g_1 (x_1), g_2 (x_1, x_2), \ldots g_m (x_1, x_2, \ldots x_m)],$$

where $P(x, x_1, x_2, \ldots. x_m)$ is a primary prime function of the h^{th} degree in x, of degrees not greater than $n_1 - 1$ in x_1, $n_2 - 1$ in x_2, $n_3 - 1$ in x_3, ... $n_m - 1$ in x_m and whose constant coefficients are rational integers.

It is easy to prove that the congruence

$$x^{p_m^h} - x \equiv 0 \; [\text{modd. } \mathfrak{p}, g_1(x_1), g_2(x_1, x_2), \ldots. g_m(x_1, x_2, \ldots. x_m)],$$

has exactly p_m^h incongruent [modd. $\mathfrak{p}$, $g_1(x_1)$, $g_2(x_1, x_2)$, ... $g_m(x_1, x_2, \ldots. x_m)$] roots.

Hence we have

$$1) \qquad x^{p_m^h} - x \equiv \prod (x - \zeta) \; [\mathfrak{p}, g_1(x_1), g_2(x_1, x_2), \ldots. g_m(x_1, x_2, \ldots. x_m)],$$

where the product is to be taken over a system of $\mathfrak{p}_m^h$ incongruent [modd. $\mathfrak{p}$, $g_1(x_1)$, $g_2(x_1, x_2)$, ... $g_m(x_1, x_2, \ldots. x_m)$] quantities which have a height h or a height d, where d is a divisor of h.

In this product, if ζ is a function of the height h, there appears as a factor the product

$$(x - \zeta)(x - \zeta^{p_m})(x - \zeta^{p_m^2}) \ldots. (x - \zeta^{p_m^{h-1}}),$$

a product which may be replaced by a primary prime function as seen above.

There appears also as a factor of the product 1), if d is a divisor of h, the product

$$(x - \zeta')(x - \zeta'^{p_m})(x - \zeta'^{p_m^2}) \ldots. (x - \zeta'^{p_m^{d-1}}),$$

where ζ' is a function which has the height d.

This product may also be replaced by a primary prime function.

It is thus evident that we may replace the product 1) by a product of primary prime functions and we have in this manner

$$x^{p_m^h} - x \equiv \prod P(x, x_1, x_2, \ldots x_m) [\text{modd. } \mathfrak{p}, g_1(x_1), g_2(x_1, x_2), \ldots g_m(x_1, x_2, \ldots x_m)],$$

where the product is to be taken over a certain number of primary prime functions.

Since every congruence between rational integers with respect to the modulus $\mathfrak{p}$, is also true when taken with respect to the modulus p, it follows, since all the coefficients in the primary prime functions are rational integers, that instead of the modular system

$$[\mathfrak{p}, g_1, (x_1), g_2(x_1, x_2), \ldots. g_m(x_1, x_2, \ldots. x_m)],$$

we may write the modular system

$$[p,\ G_1(x_1),\ G_2(x_1,\ x_2),\ \dots\ G_m(x_1,\ x_2,\ \dots\ x_m)],$$

where $G_i\ (x_1, x_2\ \dots\ x_i)$ are the resulting functions when in $g_i\ (x_1,\ x_2,\ \dots\ x_i)$ $[i = 1,\ 2,\ \dots\ m]$ we write instead of the algebraic integers $\rho_1,\ \rho_2,\ \dots\ \rho_\kappa$ which appear as coefficients the rational integers which belong to the same classes of which the integers $\rho_1,\ \rho_2,\ \dots\ \rho_\kappa$ have been taken as representatives; these rational integers are supposed reduced (mod. p).

We thus have the identical congruence

$$x^{p^h_m} - x \equiv \prod P(x, x_1, x_2, \dots x_m)[\text{modd.}\, p,\ G_1(x_1), G_2(x_1, x_2) \dots G_m(x_1 x_2 \dots x_m)],$$

where the product is taken over all primary prime functions of degree h or a divisor of h, the number of such functions being given by the formula (see p. 50):

$$p^h_m = \sum_{(d)} d\omega_d\,.$$

In this connection, attention is called to two papers by the author: 1°. *Mémoire sur les Systèmes Modulaires de Kronecker*, pp. 83 and 108, a paper which was presented as a doctor's thesis to the University of Paris and published *in extenso* in the Ann. de l'École Norm. Sup., t. XVIII. 2°. Some Remarks on Kronecker's Modular Systems, Compt. Rend. du Congrès des Mathématiciens. Paris. 1900.

I add a more general statement of a theorem first given in the above thesis, p. 42.

Let

$$1).\ [\mathfrak{p}, f_1(x),\ f_2(x),\ \dots\ f_n(x),\ h_1(x),\ h_2(x),\ \dots\ h_m(x)]$$

be a modular system in which $\mathfrak{p}$ is a prime ideal, and let the functions $f_1(x),\ f_2(x),\ \dots f_n\ (x),\ h_1(x),\ h_2(x),\ \dots\ h_m(x)$ belong to the realm $[v, x]$. Further let the functions $h_1(x),\ h_2(x),\ \dots\ h_m(x)$ be linearly dependent with respect to the modulus $\mathfrak{p}$ upon the functions $f_1\ (x), f_2(x),\ \dots\ f_n(x)$, i. e., let

$$h_i(x)\, k_i(x) = f_1(x)\, \phi_{1i}(x) + f_2(x)\, \phi_{2i}(x) + \dots + f_n(x)\, \phi_{ni}(x)\ [\text{mod. } \mathfrak{p}],$$
$$(i = 1,\ 2,\ \dots\ m),$$

where the functions $k_i(x),\ \phi_{1i}(x)\ \ \phi_{2i}(x),\ \dots\ \phi_{ni}(x)$ belong to the realm $[1, x]$.

Then, if we suppose that the functions $f_1(x), f_2(x), \ldots . f_n(x)$ are linearly independent with respect to the modulus $\mathfrak{p}$, it may be shown precisely in the same manner, as was given on p. 42 of the thesis, that the system 1) may be replaced by an equivalent system which contains only n independent elements with respect to the modulus $\mathfrak{p}$.

The theorem may be further generalized by considering functions of several variables taken with respect to the modular system $[M]$ of page 43.

UNIVERSITY OF CINCINNATI, *December* 21, 1900.